Policies and Procedures
POLICY: Risk Analysis and Management
Policy #19
Effective Date: April 2, 2014

Purpose: This policy describes the risk analysis and risk management activities that the ILHIE Authority and Participants must perform in compliance with the HIPAA Security Rule requirements.

Policy: The ILHIE Authority and Participants shall each conduct security risk assessments to identify reasonably anticipated threats and vulnerabilities that present potential risk to the confidentiality, integrity and availability of Electronic Protected Health Information requested, used or disclosed through the ILHIE. The ILHIE Authority and Participants shall each develop security risk management plans to document the issues and concerns discovered in the risk assessment process, and document recommendations for addressing these concerns through the adoption and implementation of reasonable safeguards to protect Electronic Protected Health Information created, received, maintained or transmitted using the ILHIE technology and infrastructure.

1.0 **Risk Analysis.** The ILHIE Authority and Participants shall each conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of Electronic Protected Health Information held by the ILHIE Authority or the Participant, respectively, including risks related to the use of the ILHIE.

1.1 The identification, definition and prioritization of risks to ILHIE Authority technology and infrastructure will be based on a formal, documented risk analysis process.

1.2 The ILHIE Authority and Participants shall each re-assess risks, as needed, but no less than annually, after Security Incidents, Breaches, or both and as vulnerabilities are identified, respectively.

1.3 The ILHIE Authority shall re-assess its risks whenever significant changes occur in the ILHIE's information technology environment.

2.0 **Risk Management.** The ILHIE Authority and Participants shall each implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R §164.306(a) of the HIPAA Security Rule.

2.1 Selection and implementation of such security measures will be based on a formal, documented risk management process.

2.2 The ILHIE Authority and Participant will each evaluate and maintain security measures, periodically reviewing and updating the risk management plan in response to changes and risks identified through the risk analysis process.

3.0 **Compliance.** Participants shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

3.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures, including providing documentation of the risk analysis results and risk management plan upon request.

Associated Policies & References
45 C.F.R 164.306(a)
45 C.F.R 164.308(a)(1)(ii)(A)
45 C.F.R 164.308(a)(1)(ii)(B)
Risk Management RFP

Definitions
Breach
Electronic Protected Health Information
ILHIE Authority
Participant
Security Incident